UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

SHANNON THOMAS, individually and on behalf of all others similarly situated, Plaintiff, v. **LAKEVIEW LOAN SERVICING, LLC,** Defendant.	Case No. 1:22-cv-20984 **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Plaintiff Shannon Thomas, individually, and on behalf of all others similarly situated ("Plaintiff"), through her attorneys, brings this action against Defendant Lakeview Loan Servicing, LLC ("Defendant"), and alleges upon personal knowledge as to her own actions and experiences, and upon information and belief as to all other matters, as follows:

INTRODUCTION

1. This consumer data breach arises out of Defendant's unreasonable, unlawful, and unfair practices with regard to its collection and maintenance of the highly sensitive and confidential personal and financial information of persons whose loans for which it serves as servicer, subservicer, or master servicer. Defendant's insufficient and unreasonable data security practices caused, facilitated, and exacerbated the data breach (the "Data Breach") and its impact on Plaintiff and Class members. By Defendant's own admission, the Data Breach went undetected for over a 6-week period from October 27, 2021 through December 7, 2021, and exposed the Plaintiff's and Class members' highly personally identifiable information and

financial information ("PII") to criminals, including their names, addresses, loan numbers, and Social Security numbers. For some unspecified Class members, additional loan information was also stolen by the criminals.

2. The PII that Defendant compromised, exposed, and criminals stole in the Data Breach consists of some of the most sensitive and damaging information when in the hands of criminals, including Social Security numbers, names, property information and loan numbers. Moreover, the information relates to what is for many the single most important asset, both subjectively and objectively—their home.

3. The PII stolen in the Data Breach can be used by criminals alone, and in conjunction with other pieces of information, to perpetrate crimes against Plaintiff and Class members that can result in significant liability and damage to their money, property, creditworthiness, reputation, and their ability to pay current loans, improve their credit, and/or obtain loans on favorable terms in the future.

4. Defendant is the fourth largest mortgage servicing company in the United States, servicing mortgage loans for over 1.4 million customers. This includes processing payments, managing escrow, and providing customer service in connection with mortgage loans.

5. Plaintiff and Class members entrusted Defendant, and lenders that do business with Defendant, with an extensive amount of their sensitive PII. Defendant makes public statements that it understands the importance of protecting such information. For example, in its website Privacy Policy, Defendant represents that it "recognizes the importance of keeping the personal information you provide to us private and secure," that it "use[s] the latest technology to ensure that your personal information is secure," and that it "respects your privacy".[1] In addition, Defendant represents that "[w]e maintain commercially reasonable security measures to protect

[1] https://lakeview.com/privacy-notice/ (last accessed March 30, 2022), attached as Exhibit 2.

the personal information we collect and store from loss, misuse, destruction, or unauthorized access. Our security includes physical, administrative, and technology-based measures. We use industry-standard encryption to protect data in transit and at rest. Our internal policies and procedures impose a number of standards to safeguard the confidentiality of personal information, prohibit the unlawful disclosure of personal information, and limit access to personal information." *See* Exhibit 2.

6. These representations were false. In early December 2021, Defendant learned that an unauthorized actor breached its system, accessed, and acquired electronic files containing the PII of Plaintiff and Class members. The data included, at least, Plaintiff's and Class members' first and last names, mailing addresses, loan numbers, and Social Security numbers, and in some instances "information provided in connection with a loan application, loan modification, or other items regarding loan services." *See* Notice of Data Breach ("Notice"), attached as Exhibit 1.

7. Plaintiff, individually, and on behalf of all persons similarly situated, seeks to be made whole for the losses she has incurred and will incur in the future to remedy and mitigate the risk of identity theft and fraud that the Data Breach presents. Plaintiff also seeks injunctive relief in the form of compliant data security practices, full disclosure regarding the disposition of the information in Defendant's systems, and monitoring and audits of Defendant's security practices going forward because Defendant continues to collect, maintain, and store her PII and home loan data.

PARTIES, JURISDICTION, AND VENUE

8. Plaintiff is a citizen of Ohio.

9. Defendant is a limited liability company established under the laws of the State of Delaware that maintains its headquarters and principal place of business at 4425 Ponce De Leon Blvd., 5th Floor, Coral Gables, FL 33146. The citizenship of Defendant's members is currently unknown to Plaintiff. Defendant does business in and is licensed to do business in Florida.

10. This Court has original jurisdiction under the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d)(2), because this is a Class action involving 100 or more Class members and the amount in controversy exceeds $5,000,000, exclusive of interest and costs. Many members of the Class, including Plaintiff, are citizens of different states from Defendant.

11. This Court has general personal jurisdiction over Defendant because Defendant's principal place of business is in Florida and Defendant is at home in Florida.

12. Venue is proper in this District under 28 U.S.C. §§ 1391(a)(2), 1391(b)(2), and 1391(c)(2) as a substantial part of the events giving rise to the claims emanated from activities within this District, and Defendant conducts substantial business in this District.

GENERAL ALLEGATIONS

The Data Breach

13. In its March 18, 2022, Notice sent to Plaintiff and Class members, Defendant admits that criminals accessed Defendant's file storage servicers from October 27, 2021 to December 7, 2021. *See* Exhibit 1.

14. More than three months after Defendant discovered the Data Breach and notified law enforcement, Defendant announced to impacted consumers that they were at risk of identity fraud because of its Data Breach. *See* Exhibit 1. Defendant sent notice letters to various states' Attorneys General and to at least 2,537,261 individuals affected by the Data Breach.

15. The Notice contains no header, no title, no subject line prominently indicating that it is a "Notice of Data Breach," or other title designed to grab the attention of the recipient. The first indication of "unauthorized access" comes five sentences into the otherwise unassuming letter. The letter is intentionally designed to be unremarkable and unnoticed by Plaintiff and the Class members.

16. In the Notice to Plaintiff and Class members, Defendant stated:

> A security incident involving unauthorized access to Lakeview's file servers was identified in early December 2021. Steps were immediately taken to contain the incident, notify law enforcement, and a forensic investigation firm was engaged. The investigation determined that an unauthorized person obtained access to files on Lakeview's file storage servers from October 27, 2021 to December 7, 2021.
>
> …
>
> On January 31, 2022, the review process generated a preliminary list of individuals, including you, whose name, address, loan number, and Social Security number were included in the files. We then took extensive measures to review that list to ensure accuracy and prepare the list to be used to mail notification letters. For some, the accessed files may also have included information provided in connection with a loan application, loan modification, or other items regarding loan servicing.
>
> *See* Exhibit 1.

17. Steps were not taken until late March 2022—more than three months later—to notify the impacted individuals.

18. In addition, Defendant's Notice contains misleading statements, vague statements, and material omissions. The letter raised the prospect that other items regarding Class members' loans were included in the stolen files, but did not identify what those items were or who in the Class were at risk. For instance, the letter is silent about the material issue of whether financial, bank, or payment information was accessed. As a result, Plaintiff and Class members reasonably undertook steps to mitigate, reduce, and remedy the substantial risk that the cyberattack accessed

and stole the full spectrum of their personal and financial information, which includes Social Security numbers, financial account information, loan status, balance, and payment details, and other substantial credit, financial, and personal information relating to them, their home, home loan, and creditworthiness.

19. Defendant collected, aggregated, digitized, organized, and maintained significant financial and personal information pertaining to Plaintiff, including her financial account information, name, address, contact information, and Social Security number.

20. Defendant advised in the Notice that Class members should obtain credit reports, monitor their accounts for fraudulent activity, and to maintain vigilance against the threat of identity theft or fraud.

21. As a result of the Data Breach, and as recommended by the Notice, Plaintiff and Class members have been and must continue to be vigilant and review their credit reports for incidents of identity theft, and educate themselves about security freezes, fraud alerts, and other steps to protect themselves against identity theft.

Industry Standards for Data Security

22. Defendant is aware of the importance of safeguarding Plaintiff's and Class members' PII, that its business is at risk of being targeted by hackers because of the sensitive data Defendant collects, organizes, and stores, and the foreseeable consequences of identity fraud and theft using Plaintiff's and Class members' PII if its systems are breached.

23. Because of Defendant's failure to create, maintain, and/or comply with necessary cybersecurity requirements, Defendant was unable to protect Plaintiff's and Class members' information and confidentiality, and protect against obvious and readily foreseeable threats to information security and confidentiality, and criminals gained unauthorized access to Plaintiff's

and Class members' personal and financial information in the Data Breach without being detected for weeks.

24. As the Notice reveals, only after the attack was successful did Defendant begin (if at all) to undertake the basic steps recognized in the industry to protect Plaintiff's and Class members' PII to bolster its cybersecurity posture by taking "additional steps" to "enhance [its] existing security measures." On information and belief, Defendant is circumspect about what specific measures it has taken and omits details about the Data Breach in the Notice because it intends to argue in a motion to dismiss that Plaintiff must identify what particular failures caused the Data Breach in this Complaint.

25. Defendant was unable to prevent the Data Breach, and was unable to detect the unauthorized access to its sensitive files containing protected information of more than 2 million consumers for 41 days. The allegations alone suffice to plausibly plead Defendant's security was insufficient and unreasonable for purposes of surviving a motion to dismiss. Discovery on Defendant, law enforcement investigators, and private investigators, such as Kroll, will reveal more specific facts about Defendant's deficient and unreasonable security procedures.

26. Security standards commonly accepted among businesses that store personal and financial information using the Internet include, without limitation:

a) Maintaining a secure firewall configuration;

b) Monitoring for suspicious or irregular traffic to servers;

c) Monitoring for suspicious credentials used to access servers;

d) Monitoring for suspicious or irregular activity by known users;

e) Monitoring for suspicious or unknown users;

f) Monitoring for suspicious or irregular server requests;

g) Monitoring for server requests for personal and financial information;

h) Monitoring for server requests from VPNs; and

i) Monitoring for server requests from Tor exit nodes.

28. The U.S. Federal Trade Commission ("FTC") publishes guides for businesses for cybersecurity[2] and protection of personal and financial information[3] which includes basic security standards applicable to all types of businesses.

29. The FTC recommends that businesses:

a) Identify all connections to the computers where you store sensitive information;

b) Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks;

c) Do not store sensitive consumer data on any computer with an internet connection unless it is essential for conducting their business;

d) Scan computers on their network to identify and profile the operating system and open network services. If services are not needed, they should be disabled to prevent hacks or other potential security problems. For example, if email service or an internet connection is not necessary on a certain computer, a business should consider closing the ports to those services on that computer to prevent unauthorized access to that machine;

e) Pay particular attention to the security of their web applications—the software used to give information to visitors to their websites and to retrieve information from them. Web applications may be particularly vulnerable to a variety of hack attacks;

f) Use a firewall to protect their computers from hacker attacks while it is connected to a network, especially the internet;

g) Determine whether a border firewall should be installed where the business's network connects to the internet. A border firewall separates the

[2] *See* F.T.C., *Start with Security: A Guide for Business*, (June 2015), https://www.ftc.gov/system/files/ documents/plain-language/pdf0205-startwithsecurity.pdf (*last accessed* July 23, 2020).

[3] *See* F.T.C., *Protecting Personal Information: A Guide for Business*, (Oct. 2016), https://www.ftc.gov/ system/files/documents/plain-language/pdf-0136_protecting personalinformation.pdf (*last accessed* July 23, 2020).

network from the internet and may prevent an attacker from gaining access to a computer on the network where sensitive information is stored. Set access controls—settings that determine which devices and traffic get through the firewall—to allow only trusted devices with a legitimate business need to access the network. Since the protection a firewall provides is only as effective as its access controls, they should be reviewed periodically;

h) Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than-average traffic at unusual times of the day, and

i) Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from their system to an unknown user. If large amounts of information are being transmitted from a business' network, the transmission should be investigated to make sure it is authorized.

30. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer information, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.[4]

31. Because Defendant was entrusted with consumers' personal and financial information, it had, and has, a duty to keep their personal and financial information secure.

32. Plaintiff and Class members reasonably expect that when they provide their personal and financial information to a company, the company will safeguard their personal and financial information.

[4] F.T.C., *Privacy and Security Enforcement: Press Releases*, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement (*last accessed* July 15, 2020).

33. Nonetheless, Defendant failed to upgrade and maintain its data security systems in a meaningful way so as to prevent the Data Breach.

34. Specifically, in breach of its duties, Defendant failed to:

a) Replace email filtering tools, malware software, and Internet monitoring tools with more robust solutions that utilize artificial intelligence ("AI") to detect and block known and newly introduced malware;

b) Block all inbound and outbound Internet, email, and network traffic to foreign countries;

c) Maintain a secure firewall configuration;

d) Monitor for suspicious or irregular traffic to servers;

e) Monitor for suspicious credentials used to access servers;

f) Monitor for suspicious or irregular activity by known users;

g) Monitor for suspicious or unknown users;

h) Monitor for suspicious or irregular server requests;

i) Monitor for server requests for personal and financial information;

j) Monitor for server requests from VPNs;

k) Monitor for server requests from Tor exit nodes;

l) Identify all connections to the computers where Defendant stores sensitive information;

m) Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks;

n) Scan computers on Defendant's network to identify and profile the operating system and open network services, and disable services that are not needed to prevent hacks or other potential security problems;

o) Pay particular attention to the security of Defendant's web applications—the software used to give information to visitors to its websites and to retrieve information from them;

p) Use a firewall to protect Defendant's computers from hacker attacks while it is connected to a network, especially the Internet;

q) Determine whether a border firewall should be installed where Defendant's network connects to the Internet;

r) Monitor incoming traffic for signs that someone is trying to hack in, and

s) Monitor outgoing traffic for signs of a data breach.

35. Had Defendant properly maintained its systems and adequately protected them, it could have prevented the Data Breach.

Defendant Owed a Duty to Plaintiff and Class Members to Adequately Safeguard Their PII

36. Defendant is aware of the importance of security in maintaining personal information (particularly sensitive personal and financial information), and the value its users and clients place on keeping their PII secure.

37. Defendant owes a duty to Plaintiff and the Class members to maintain adequate security and to protect the confidentiality of their PII.

38. Defendant owes a further duty to its customers to immediately and accurately notify them of a breach of its systems to protect them from identity theft and other misuse of their personal data and to take adequate measures to prevent further breaches.

The Categories of PII at Issue Here Are Particularly Valuable to Criminals

39. Businesses that store sensitive PII are likely to be targeted by cyber criminals. Credit card and bank account numbers are tempting targets for hackers. However, information such as dates of birth and Social Security numbers are even more attractive to hackers; they are not easily destroyed and can be easily used to perpetrate identity theft and other types of fraud.

40. The unauthorized disclosure of Social Security numbers can be particularly damaging, because Social Security numbers cannot easily be replaced. In order to obtain a new

Social Security number a person must prove, among other things, that he or she continues to be disadvantaged by the misuse. Thus, no new Social Security number can be obtained until the damage has been done.

41. Furthermore, as the Social Security Administration ("SSA") warns:

> Keep in mind that a new number probably will not solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number will not guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.
>
> If you receive a new Social Security Number, you should not be able to use the old number anymore.
>
> For some victims of identity theft, a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under the new number may make more difficult for you to get credit.[5]

42. Here, the unauthorized access by the hackers left the cyber criminals with the tools to perform the most thorough identity theft—they have obtained all the essential PII to mimic the identity of the user. Plaintiff's and Class members' stolen personal data represents essentially one-stop shopping for identity thieves.

43. According to the FTC, identity theft wreaks havoc on consumers' finances, credit history, and reputation and can take time, money, and patience to resolve.[6] Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities

[5] SSA, Identity Theft and Your Social Security Number, SSA Publication No. 05-10064 (Dec. 2013), *available at* http://www.ssa.gov/pubs/EN-05-10064.pdf (last visited 3/26/2021).

[6] *See Taking Charge, What to Do If Your Identity is Stolen*, FTC, 3 (2012), http://www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf (last visited 3/26/2021).

fraud, and bank and finance fraud.[7]

44. More recently the FTC has released its updated publication on protecting PII for businesses, which includes instructions on protecting PII, properly disposing of PII, understanding network vulnerabilities, implementing policies to correct security problems, using intrusion detection programs, monitoring data traffic, and having in place a response plan.

45. The FTC has, upon information and belief, brought enforcement actions against businesses for failing to protect PII. The FTC has done this by treating a failure to employ reasonable measures to protect against unauthorized access to PII as a violation of the FTC Act, 15 U.S.C. § 45.

46. General policy reasons support such an approach. A person whose personal information has been compromised may not see any signs of identity theft for *years*. According to the GAO Report:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[8]

47. Companies recognize that PII is a valuable asset. Indeed, PII is a valuable commodity. A "cyber black-market" exists in which criminals openly post stolen Social Security numbers and other PII on a number of Internet websites. Plaintiff's and Class members' personal data that was stolen has a high value on both legitimate and black markets.

---

[7] *Id.* The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 CFR § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." *Id*.

[8] *See* http://www.gao.gov/new.items/d07737.pdf at 29 (last visited 11/13/2020).

48. At an FTC public workshop in 2001, then-Commissioner Orson Swindle described the value of a consumer's personal information as follows:

> The use of third party information from public records, information aggregators and even competitors for marketing has become a major facilitator of our retail economy. Even [Federal Reserve] Chairman [Alan] Greenspan suggested here some time ago that it's something on the order of the life blood, the free flow of information.[9]

49. Individuals rightfully place a high value not only on their PII, but also on the privacy of that data. Researchers have already begun to shed light on how much individuals value their data privacy – and the amount is considerable.

50. Notably, one study on website privacy determined that U.S. consumers valued the restriction of improper access to their personal information – the very injury at issue here – between $11.33 and $16.58 per website. The study also determined that "[a]mong U.S. subjects, protection against errors, improper access, and secondary use of personal information is worth US$30.49 – 44.62."[10] This study was done in 2002. The sea-change in how pervasive the Internet is in everyday lives since then indicates that these values—when associated with the loss of PII to bad actors—would be exponentially higher today.

51. Identity thieves may commit various types of crimes such as immigration fraud, obtaining a driver's license or identification card in the victim's name but with another's picture, and/or using the victim's information to obtain a fraudulent tax refund or fraudulent unemployment benefits. The United States government and privacy experts acknowledge that it may take years for identity theft to come to light and be detected.

---

[9] FEDERAL TRADE COMMISSION, *The Information Marketplace: Merging and Exchanging Consumer Data*, *transcript available* at http://www.ftc.gov/news-events/events-calendar/2001/03/information-marketplace-merging-exchanging-consumer-data (last visited 11/13/2020).

[10] Hann, Hui, *et al*, The Value of Online Information Privacy: Evidence from the USA and Singapore, at 17. Oct. 2002, available at https://www.comp.nus.edu.sg/~ipng/research/privacy.pdf (last visited 3/26/2021).

52. As noted above, the disclosure of Social Security numbers in particular poses a significant risk. Criminals can, for example, use Social Security numbers to create false bank accounts or file fraudulent tax returns.[11] Plaintiff and Class members will and already have spent time contacting various agencies, such as the Internal Revenue Service and the Social Security Administration. They also now face a real and imminent substantial risk of identity theft and other problems associated with the disclosure of their Social Security number and will need to monitor their credit and tax filings for an indefinite duration.

53. Again, because the information Defendant allowed to be compromised and taken is of such a durable and near-permanent quality, the harms to Plaintiff and the Class will continue to grow, and Plaintiff and the Class will continue to be at substantial risk for further imminent and future harm.

Damages From Data Breaches

54. According to Javelin Strategy & Research, in 2017 alone over 16.7 million individuals were affected by identity theft, causing $16.8 billion to be stolen.

55. Consumers place a high value not only on their personal and financial information, but also on the privacy of that data. This is because identity theft causes "significant negative financial impact on victims" as well as severe distress and other strong emotions and physical reactions.

56. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report"). The GAO Report explains that "[t]he term 'identity theft' is broad and encompasses many types of criminal activities, including fraud on existing accounts—such as unauthorized use of a stolen credit card number—or fraudulent creation of

[11] When fraudulent tax returns are filed, the requirements for a legitimate taxpayer to file their tax returns with the IRS increase, including the necessity to obtain and utilize unique PIN numbers just to be able to file a tax return.

new accounts—such as using stolen data to open a credit card account in someone else's name." *See In re Zappos.com, Inc.*, 888 F.3d 1020, 1024 (9th Cir. 2018) (quoting the GAO Report). The GAO Report notes that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."

57. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports often, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.

58. Identity thieves use stolen personal and financial information for "various types of criminal activities, such as when personal and financial is used to commit fraud or other crimes," including "credit card fraud, phone or utilities fraud, bank fraud and government fraud." *In re Zappos.com, Inc.*, 888 F.3d at 1024. The information exfiltrated in the Data Breach can also be used to commit identity theft by placing Plaintiff and Class members at a higher risk of "phishing," "vishing," "smishing," and "pharming," which are which are ways for hackers to exploit information they already have to get even more personally identifying information through unsolicited email, text messages, and telephone calls purportedly from a legitimate company requesting personal, financial, and/or login credentials.

59. There may be a time lag between when harm occurs versus when it is discovered, and also between when personal and financial information is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.
>
> *See* GAO Report, at p. 29.

60. Personal and financial information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber blackmarket" for years.

61. Thus, there is a strong probability that entire batches of stolen information have been dumped on the black market, or are yet to be dumped on the black market, meaning Plaintiff and Class members are at an increased risk of fraud and identity theft for many years into the future.

62. Data breaches are preventable. As Lucy Thompson wrote in the DATA BREACH AND ENCRYPTION HANDBOOK, "In almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions." She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised . . . ."

63. "Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures. . . . Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a data breach never occurs."

64. The types of information Defendant acknowledges were stolen by the criminals are sufficiently sensitive and valuable to identity thieves and criminals in perpetrating identity

crimes. Defendant states that Plaintiff's and all Class members' names, address, loan numbers, and Social Security numbers were exposed. This information is essentially immutable and can be used to perpetrate scams, victimize the persons who own the information, and commit identity theft and fraud.

65. The types of information compromised in the Data Breach are immutable. Plaintiff and Class members are not able to change them or simply cancel them, like a credit card, to avoid harm or fraudulent use of the information. Just like a birthdate or a mother's maiden name, these pieces of information cannot be changed by logging into a website and changing them in settings, and they can be used alone or in conjunction with other pieces of information to commit serious fraud.

66. Criminals can use the information to devise and employ phishing and social engineering schemes capitalizing on the genuine information stolen from Defendant to send fraudulent mail, emails, and other communications to Plaintiff and Class members that look authentic, but which are designed to lure them into paying money or providing other information that the criminals can use to steal money. For example, homeowners with trouble paying their loan payments may experience scams targeting them.

67. According to Experian:[12]

> Mortgage Foreclosure Relief and Debt Management Scams
>
> In this type of mortgage fraud, scammers contact homeowners offering help if they can't make payments or may be falling behind on their mortgage (the primary contact is by phone with these). … Often they make promises of lower payments or making the payments for a homeowner in exchange for rent payments to their company. However, they don't actually make the mortgage payments and you may end up going into foreclosure anyway.

12 https://www.experian.com/blogs/ask-experian/heres-everything-you-need-to-know-about-the-risks-of-mortgage-fraud/ (last visited March 30, 2022).

> Also known as foreclosure scams or foreclosure rescue schemes, this kind of fraud is unfortunately very common and can cost consumers a lot of Money.

68. The information stolen in the Data Breach, by itself, can also be used by criminals to perpetrate fraud that will leave Plaintiff and Class members holding the bag. Experian explains that certain scams, including mortgage fraud, can be effectively perpetrated using only a name and loan number.[13]

> How Consumers Are Affected By Mortgage Fraud
>
> Identity theft is a particularly threatening form of mortgage fraud, as it tends to lead directly toward homeowner financial loss. For example, if an identity thief steals a homeowner's Social Security number, or intercepts the mortgage account number, he or she can use that information to take out a home equity line of credit (also known as a HELOC) worth tens of thousands of dollars, in the homeowner's name.

69. Experian explains how mortgage fraud impacts the homeowner. When the credit is provided to the fraudster:[14]

> The cash is sent to a fraudulent account established by the thief, and the homeowner is left holding the bill. Or, the fraudster could take out a second mortgage using the homeowner's stolen data information, and escape with the cash, once again leaving the debt to the homeowner.
>
> While any form of mortgage fraud is a serious offense, losing one's data to identity thieves can trigger a financial loss that's difficult to overcome, and that could take years to clear. Additional impacts include losing money, time, or missing out on the purchase of a dream home because you have to take additional time to deal with restoring your identity if you're the victim of mortgage fraud.

70. Identity Force explains what a thief or scammer can do with sensitive information, such as loan information and identifying details, including stealing your home:[15]

> Mortgaging Your Good Name

[13] *Id.*
[14] *Id.*
[15] https://www.identityforce.com/blog/home-loan-identity-theft. (last visited March 30, 2022)

> Mortgage fraud through identity theft is a very real risk. A thief can steal your Social Security number and other identifying details, then pretend to be you to a bank or mortgage broker. The criminal might refinance your home for more than what's owed and then take the extra cash or obtain a home equity line of credit and drain that account.
>
> In some cases, you can experience house stealing through a fraudulent deed transfer. An identity thief could use stolen information to execute a transfer, which would put your property in his or her name. That means you'd legally no longer own that real estate. Since the criminal's name is on the deed, he or she would have the right to take out loans against the house. With no payments made on those loans or the mortgage, the property could even go into foreclosure.
>
> Thieves can get the information they need for these transactions by stealing your mail, getting personal details through fraudulent phone calls, or making copies of your driver's license to impersonate you. Unfortunately, sometimes it's friends and family who are the culprits (known as familiar fraud) since they may have access to files inside a home and often know many of the personal details required to impersonate you.

Plaintiff Received Defendant's Data Breach Notification Letter

71. Plaintiff took out a mortgage loan for property in Ohio. For all times relevant to this Complaint, Defendant was the servicer of Plaintiff's mortgage loan.

72. Plaintiff and Class members provided their lenders and Defendant with significant personal, income, and financial information that Defendant was able to acquire and to supplement by obtaining credit reports and banking information from third parties. Such information included, but is not limited to:

- Full name, mailing address, phone numbers, email address, and loan identification number;
- Co-borrower contact information, phone numbers, email address, and mailing address;
- Notations and comments concerning collections and loan servicing;
- Fee balance information;

- Information regarding insurance on the property and property details pertinent thereto;
- Loan history information, Social Security number, transaction dates, due dates, transaction amount, principal amount, end principal balance, interest, escrow amounts, check numbers, late charges, assistance amounts; details on loans in arrears;
- Tax information, including tax type, frequency, account number, and payee information;
- Credit information from consumer reports and files held by consumer reporting agencies; and
- Other information, but Plaintiff does not know the full extent of the information Defendant has relating to him.

73. It is plausible to assume that the foregoing pieces of information relating to Plaintiff and Class members were exposed, compromised, accessed, viewed without authorization, and stolen in the Data Breach by criminals. Defendant's Notice indicates that additional loan information was stolen, but has not described what that information entailed or whose information was stolen.

74. On or about March 18, 2022, Defendant sent the Notice by mail notifying Plaintiff that her personal and financial information, including her name, address, loan number and Social Security number, and perhaps additional loan information, had been accessed and stolen in the Data Breach at least three months earlier. An example of the Notice that Plaintiff received is attached as Exhibit 1.

75. The Notice also provided Plaintiff with steps to take to protect her personal information. After explaining that Plaintiff's personal information was taken by criminals and explaining that a comprehensive investigation was in process, Defendant provided some boilerplate suggestions to Plaintiff on how to immediately report any suspicious activity, and obtain credit reports from each nationwide credit reporting agency.

76. As a direct result of the Data Breach and the unreasonably delayed Notice, Plaintiff has already had to spend time and energy protecting and monitoring her identity and credit, spent at least one hour reviewing bank accounts and statements, spent at least one hour changing passwords related to her business and personal accounts, spent at least 30 minutes reviewing her credit reports from all three credit bureaus, and she will have to spend additional time and energy in the future continuing to monitor and protect her identity and credit. As a direct result of the Data Breach, Plaintiff has suffered anxiety, emotional distress, and loss of privacy. Additionally, after receiving the Notice, Plaintiff purchased Lifelock Advantage, an identity theft protection product, for $15.99 a month.

Plaintiff's and Class Members' Damages

77. As a direct and proximate result of Defendant's conduct, Plaintiff and the Class members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

78. Plaintiff and members of the Class have or will suffer actual injury as a direct result of the Data Breach including:

a) Spending time reviewing finding fraudulent charges and remedying fraudulent charges;

b) Purchasing credit monitoring and identity theft prevention;

c) Time and money addressing and remedying identity theft;

d) Spending time placing "freezes" and "alerts" with credit reporting agencies and, subsequently, temporarily lifting a security freeze on a credit report, or removing a security freeze from a credit report;

e) Spending time on the phone with or visiting financial institutions to dispute fraudulent charges;

f) Contacting their financial institutions and closing or modifying financial accounts compromised as a result of the Data Breach; and

g) Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

82. Moreover, Plaintiff and the Class members have an interest in ensuring that their personal and financial information is protected from further breaches by the implementation of security measures and safeguards, including making sure that the storage of data containing their personal and financial information is secure.

83. As a direct and proximate result of Defendant's actions and inactions, Plaintiff and Class members have suffered anxiety, emotional distress, and loss of privacy.

84. As a direct and proximate result of Defendant's actions and inactions, Plaintiff and Class members are at an increased and immediate risk of future harm, including from identity theft and fraud related to their financial accounts.

85. As a result of the Data Breach, Plaintiff and Class members are at an imminent risk of identity theft and fraud. This risk will continue to exist for years to come, as Plaintiff and Class members must spend their time being extra vigilant, due to Defendant's failures, to try to prevent being victimized for the rest of their lives.

86. Because Defendant presented such an easy target to cyber criminals, Plaintiff and Class members have already been subjected to violations of their privacy, and have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiff and Class members must now and in the future, spend time to more closely monitor their financial accounts to guard against identity theft and other fraud.

87. Plaintiff and Class members may also incur out-of-pocket costs for, among other things, purchasing credit monitoring services or other protective measures to deter and detect identity theft. After receiving the Notice, Plaintiff purchased Lifelock Advantage, an identity theft protection product, for $15.99 a month.

Application of Florida Law to
The Claims of Plaintiff and the Class

88. Florida has a significant interest in regulating the conduct of businesses operating within its borders and commerce that takes place in Florida. Florida seeks to protect the rights and interests of all Florida residents and citizens of the United States against a company with its principal place of business in Florida. Florida has a greater interest in the claims of Plaintiff and members of the Class than their home states, and is most intimately concerned with the claims and outcome of this litigation.

89. Application of Florida law to the Class with respect to Plaintiff's and Class members' claims is neither arbitrary nor fundamentally unfair because Florida has significant contacts and a significant aggregation of contacts that create a state interest in the claims of Plaintiff and the Class.

90. The Data Breach occurred on systems located in Florida.

91. The decisions of Defendant regarding data collection practices, data security protocols, Data Breach response measures, the forensic investigation into the Data Breach, and Defendant's preparation of the notification all occurred in Florida.

92. Plaintiff and Class members sent money either to the Defendant directly, or to the Defendant via payments to Defendant's sub-servicer who would then tender payment to Defendant in Florida, in connection with Defendant's role as their home loan servicer.

93. The hacker(s) gained unauthorized access to Plaintiff's and Class members' PII in Florida. Therefore, Plaintiff and Class members suffered injury in Florida.

94. Numerous courts have recognized a growing trend of applying the law of state where the Data Breach occurred over the law of the state where the plaintiffs happen to reside. *See, e.g.*, *Schmitt v. SN Servicing Corp.*, No. 21-cv-03355-WHO, 2021 WL 3493754, at *3 (N.D.

Cal. Aug. 9, 2021); *In re Premera Blue Cross Customer Data Sec. Breach Litig.*, No. 3:15-MD-2633-SI, 2019 WL 3410382, at *14 (D. Or. Jul 29, 2019); *First Choice Fed. Credit Union v. Wendy's Co.*, No CV 16-506, 2018 WL 2729264, at *6–7 (W.D Pa. May 9, 2018); *In re Target Corp. Customer Data Sec. Breach Litig.*, 309 F.R.D. 482, 486 (D. Minn. Sept 15, 2015).

95. Under Florida's choice of law principles, the law of Florida applies to the claims of Plaintiff and Class members.

CLASS ACTION ALLEGATIONS

92. Plaintiff brings this action pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3) on behalf of a class of similarly situated individuals (the "Class") defined as follows:

> All individuals in the United States whose personally identifiable information was compromised in the Data Breach.

93. In addition, Plaintiff brings this action pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3) on behalf of a subclass of similarly situated individuals in Ohio ("Ohio Subclass") defined as follows:

> All individuals in Ohio whose personally identifiable information was compromised in the Data Breach.

94. Excluded from the Class and Ohio Subclass (collectively, "Classes") are Defendant; any entity in which Defendant has a controlling interest, is a parent or subsidiary, or which is controlled by Defendant; and the affiliates, legal representatives, attorneys, heirs, predecessors, successors, and assigns of Defendant. Also excluded are the judges and court personnel in this case and any members of their immediate families.

95. Plaintiff reserves the right to modify and/or amend the Class and Ohio Subclass definition, including but not limited to creating subclasses, as necessary.

96. ***Numerosity***. The Classes are so numerous that joinder of all members is impracticable. The Class includes at least 2,537,261 individuals whose PII was compromised in

the Data Breach. The identities of all Class members are ascertainable through Defendant's records.

97. ***Commonality***. There are numerous questions of law and fact common to Plaintiff and the Class, including the following:

- Whether and to what extent Defendant had a duty to protect the PII of Plaintiff and Class members;
- Whether Defendant had a duty not to disclose the PII of Plaintiff and Class members to unauthorized third parties;
- Whether Defendant had a duty not to use the PII of Plaintiff and Class members for non-business purposes;
- Whether Defendant failed to adequately safeguard the PII Plaintiff and Class members;
- Whether and when Defendant actually learned of the Data Breach;
- Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class members that their PII had been compromised;
- Whether Defendant violated the law by failing to promptly notify Plaintiff and Class members that their PII had been compromised;
- Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;
- Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiff and Class members;
- Whether Plaintiff and Class members are entitled to actual damages, nominal damages, and/or exemplary damages as a result of Defendant's wrongful conduct;
- Whether Plaintiff and Class members are entitled to restitution as a result of Defendant's wrongful conduct; and
- Whether Plaintiff and Class members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

98. ***Typicality***. Plaintiff's claims are typical of the claims of the Class in that Plaintiff, like all Class members, had her personal data compromised, breached and stolen in the Data Breach. Plaintiff and Class members were injured through Defendant's uniform misconduct described in this Complaint and assert the same claims for relief.

99. ***Adequacy***. Plaintiff and counsel will fairly and adequately protect the interests of the Class. Plaintiff has retained counsel who are experienced in class actions and complex litigation, including data privacy litigation of this kind. Plaintiff has no interests that are antagonistic to, or in conflict with, the interests of other members of the Class.

100. ***Predominance***. The questions of law and fact common to Class members predominate over any questions which may affect only individual members.

101. ***Superiority***. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Moreover, absent a class action, most Class members would find the cost of litigating their claims prohibitively high and would therefore have no effective remedy, so that in the absence of class treatment, Defendant's violations of law inflicting substantial damages in the aggregate would go unremedied without certification of the Class. Plaintiff and Class members have been harmed by Defendant's wrongful conduct and/or action. Litigating this action as a class action will reduce the possibility of repetitious litigation relating to Defendant's conduct and/or inaction. Plaintiff knows of no difficulties that would be encountered in this litigation that would preclude its maintenance as a class action.

102. Class certification, therefore, is appropriate under Fed. R. Civ. P. 23(b)(3), because the above common questions of law or fact predominate over any questions affecting

individual members of the Class, and a class action is superior to other available methods for the fair and efficient adjudication of this controversy.

103. Class certification is appropriate under Fed. R. Civ. P. 23(b)(2), because Defendant has acted or refused to act on grounds that apply generally to the class so that final injunctive relief or corresponding declaratory relief is appropriate respecting the class as a whole.

FIRST CAUSE OF ACTION
Negligence
(On behalf of Plaintiff and the Class)

104. Plaintiff repeats and realleges the allegations of paragraphs 1-103 with the same force and effect as though fully set forth herein.

105. Defendant's actions and inactions were of the type that would result in foreseeable, unreasonable risk of harm to Plaintiff and Class members. Defendant knew, or should have known, of the risks inherent in collecting and storing the personal and financial information of Plaintiff and Class members and the importance of adequate security in storing the information. Additionally, Defendant was well aware of numerous, well-publicized data breaches that exposed the personal and financial information of individuals.

106. Defendant had a common law duty to prevent foreseeable harm to Plaintiff's and Class members' PII. This duty existed because Plaintiff and Class members were the foreseeable and probable victims of the failure of Defendant to adopt, implement, and maintain reasonable security measures so that Plaintiff's and Class members' personal and financial information would not be unsecured and accessible by unauthorized persons.

107. Defendant had a special relationship with Plaintiff and Class members. Defendant was entrusted with Plaintiff's and Class members' personal and financial information, and

Defendant was in a position to protect the personal and financial information from unauthorized access.

108. As a mortgage loan servicer, Defendant is not chosen by the borrower to service loans or to safeguard the borrower's personal information; instead, Defendant is chosen by their lender. A borrower whose loan is serviced by Defendant is a captive customer of Defendant. Borrowers do not have the opportunity to move their account to a different mortgage loan servicer because of concerns about Defendant's ability to protect their private and sensitive personal financial information.

109. The duties of Defendant also arose under section 5 of the FTC Act, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect individuals' personal and financial information by companies. Various FTC publications and data security breach orders further form the basis of the duties of Defendant.

110. Defendant had a duty to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Plaintiff's and Class members' personal and financial information in its possession so that the personal and financial information would not come within the possession, access, or control of unauthorized persons.

111. More specifically, the duties of Defendant included, among other things, the duty to:

- Adopt, implement, and maintain adequate security measures for protecting an individual's personal and financial information to ensure that the information is not accessible online by unauthorized persons;
- Adopt, implement, and maintain adequate security measure for deleting or destroying personal and financial information when Defendant's business needs no longer required such information to be stored and maintained; and

- Adopt, implement, and maintain processes to quickly detect a data breach and to promptly act on warnings about data breaches, and notify affected persons without unreasonable delay.

112. Defendant breached the foregoing duties to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting individual's personal and financial information in its possession so that the information would not come within the possession, access, or control of unauthorized persons.

113. Defendant acted with reckless disregard for the security of the personal and financial information of Plaintiff and the Class because Defendant knew or should have known that its data security was not adequate to safeguard the personal and financial information that was collected and stored.

114. Defendant acted with reckless disregard for the rights of Plaintiff and the Class members by failing to promptly detect the Data Breach, and further, by failing to notify Plaintiff and the Class members of the Data Breach in the most expedient time possible and without unreasonable delay pursuant to common law duties to provide reasonably timely and truthful data-breach notification, so that Plaintiff and Class members could promptly take measures to protect themselves from the consequences of the unauthorized access to the personal and financial information compromised in the Data Breach.

115. As a result of the conduct of Defendant, Plaintiff and Class members have suffered and will continue to suffer foreseeable harm. Plaintiff and Class members have suffered actual damages including, but not limited to, imminent risk of identity theft; expenses and/or time spent on credit monitoring for a period of years; time spent scrutinizing bank statements, credit card statements, and credit reports; time spent initiating fraud alerts and credit freezes and

subsequently temporarily lifting credit freezes; and increased risk of future harm. Further, Plaintiff and Class members have suffered and will continue to suffer other forms of injury and/or harm including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

SECOND CAUSE OF ACTION
Negligence Per Se
(On Behalf of Plaintiff and the Class)

116. Plaintiff repeats and reallege the allegations of paragraphs 1-103 with the same force and effect as though fully set forth herein.

117. "Section 5 of the FTC Act [15 U.S.C. § 45] is a statute that creates enforceable duties, and this duty is ascertainable as it relates to data breach cases based on the text of the statute and a body of precedent interpreting the statute and applying it to the data beach context." *In re Capital One Consumer Data Sec. Breach Litig.*, 488 F. Supp. 3d 374, 407 (E.D. Va. 2020). "For example, in *F.T.C. v. Wyndham Worldwide Corp.*, 799 F.3d 236, 240 (3d Cir. 2015), the United States Court of Appeals for the Third Circuit affirmed the FTC's enforcement of Section 5 of the FTC Act in data breach cases." *Capital One Data Security Breach Litigation*, 488 F. Supp. 3d at 407.

118. In addition, Plaintiff and Class members may maintain a negligence per se claim based on conduct declared unlawful under the Safeguards Rule, 16 C.F.R. part 314, promulgated by the FTC pursuant to authority delegated by Congress under the Gramm-Leach-Bliley Act, 15 U.S.C. § 6801(b), to establish standards for financial institutions relating to administrative, technical, and physical safeguards for nonpublic information, including Plaintiff's and Class members' PII.

119. The Safeguards Rule at 16 C.F.R. § 314.4 provides:

In order to develop, implement, and maintain your information security program, [a financial institution] shall:

(a) Designate an employee or employees to coordinate your information security program.

(b) Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks. At a minimum, such a risk assessment should include consideration of risks in each relevant area of your operations, including:

(1) Employee training and management;

(2) Information systems, including network and software design, as well as information processing, storage, transmission and disposal; and

(3) Detecting, preventing and responding to attacks, intrusions, or other systems failures.

(c) Design and implement information safeguards to control the risks you identify through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.

(d) Oversee service providers, by:

(1) Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue; and

(2) Requiring your service providers by contract to implement and maintain such safeguards.

(e) Evaluate and adjust your information security program in light of the results of the testing and monitoring required by paragraph (c) of this section; any material changes to your operations or business arrangements; or any other circumstances that you know or have reason to know may have a material impact on your information security program.

16 C.F.R. § 314.4.

120. The Safeguards Rule is a process-based rule drafted using intentionally broad language and not incorporating any specific information security standard or framework to allow financial institutions flexibility to "shape the information security programs to their particular business and to allow the programs to adapt to changes in technology and threats to the security and integrity of customer information."[16]

121. Defendant was and is a financial institution.

122. Plaintiff's and Class members' PII was and is nonpublic personal information and customer information.

123. Defendant committed unlawful acts by failing to comply with the requirements of

[16] Fed. Trade Comm'n, Standards for Safeguarding Customer Information, 84 Fed. Reg. 13158, 13159 (Apr. 4, 2019), also available at https://www.federalregister.gov/documents/2019/04/04/2019-04981/standards-for-safeguarding-customer- information (last visited Nov. 16, 2021).

the Safeguards Rule, including but not limited to, failing to:

- Upgrade and maintain its data security systems in a meaningful way so as to prevent the Data Breach;
- Replace email filtering tools, malware software, and Internet monitoring tools with more robust solutions that utilize artificial intelligence ("AI") to detect and block known and newly introduced malware;
- Block all inbound and outbound Internet, email, and network traffic to foreign countries;
- Maintain a secure firewall configuration;
- Monitor for suspicious or irregular traffic to servers;
- Monitor for suspicious credentials used to access servers;
- Monitor for suspicious or irregular activity by known users;
- Monitor for suspicious or unknown users;
- Monitor for suspicious or irregular server requests;
- Monitor for server requests for personal and financial information;
- Monitor for server requests from VPNs;
- Monitor for server requests from Tor exit nodes;
- Identify all connections to the computers where Defendant stores sensitive information;
- Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks;
- Scan computers on Defendant's network to identify and profile the operating system and open network services, and disable services that are not needed to prevent hacks or other potential security problems;
- Pay particular attention to the security of Defendant's web applications—the software used to give information to visitors to its websites and to retrieve information from them;
- Use a firewall to protect Defendant's computers from hacker attacks while it is connected to a network, especially the Internet;
- Determine whether a border firewall should be installed where Defendant's network connects to the Internet;

- Monitor incoming traffic for signs that someone is trying to hack in;
- Monitor outgoing traffic for signs of a data breach;
- Identify all connections to the computers where you store sensitive information;
- Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks;
- Not store sensitive consumer data on any computer with an internet connection unless it is essential for conducting their business;
- Scan computers on their network to identify and profile the operating system and open network services. If services are not needed, they should be disabled to prevent hacks or other potential security problems. For example, if email service or an internet connection is not necessary on a certain computer, a business should consider closing the ports to those services on that computer to prevent unauthorized access to that machine;
- Pay particular attention to the security of their web applications—the software used to give information to visitors to their websites and to retrieve information from them. Web applications may be particularly vulnerable to a variety of hack attacks;
- Use a firewall to protect their computers from hacker attacks while it is connected to a network, especially the internet;
- Determine whether a border firewall should be installed where the business's network connects to the internet. A border firewall separates the network from the internet and may prevent an attacker from gaining access to a computer on the network where sensitive information is stored. Set access controls—settings that determine which devices and traffic get through the firewall—to allow only trusted devices with a legitimate business need to access the network. Since the protection a firewall provides is only as effective as its access controls, they should be reviewed periodically;
- Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than-average traffic at unusual times of the day; and
- Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from their system to an unknown user. If large amounts of information are being transmitted from a business' network, the transmission should be investigated to make sure it is authorized.

124. Plaintiff and Class members are in the group of persons the FTC Act and Safeguards Rule were enacted and implemented to protect, and the harms they suffered in the Data Breach as a result of Defendant's violations of the FTC Act and Safeguards Rules were the types of harm they designed to prevent.

125. As a result of the conduct of Defendant that violated the FTC Act and the Safeguards Rule, Plaintiff and Class members have suffered and will continue to suffer foreseeable harm. Plaintiff and Class members have suffered actual damages including, but not limited to, imminent risk of identity theft; expenses and/or time spent on credit monitoring for a period of years; time spent scrutinizing bank statements, credit card statements, and credit reports; time spent initiating fraud alerts and credit freezes and subsequently temporarily lifting credit freezes; and increased risk of future harm. Further, Plaintiff and Class members have suffered and will continue to suffer other forms of injury and/or harm including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

THIRD CAUSE OF ACTION
Violation of Florida Deceptive and Unfair Trade Practices Act,
Fla Stat. § 501.201, *et seq.*
(On Behalf of Plaintiff and the Class)

126. Plaintiff repeats and realleges paragraphs 1-103 with the same force and effect as though fully set forth herein.

127. Plaintiff and Class members are consumers, as defined by Fla. Stat. § 501.203.

128. Defendant advertised, offered, or sold goods or services in Florida and engaged in trade or commerce directly or indirectly affecting the people of Florida.

129. Defendant engaged in unconscionable, unfair, and deceptive acts and practices in the conduct of trade and commerce, in violation of Fla. Stat. § 501.204(1), including:

- Failing to implement and maintain reasonable security and privacy measures

to protect Plaintiff's and Class members' PII, which was a direct and proximate cause of the Data Breach;

- Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures in response to industry standards and best practices, which directly caused the Data Breach;
- Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class members' PII, including duties imposed by the FTC Act and the Safeguards Rule, which directly caused the Data Breach;
- Misrepresenting that Defendant would protect the privacy and confidentiality of Plaintiff's and Class members' PII, including by implementing and maintaining reasonable security measures, which directly caused the Data Breach;
- Misrepresenting that Defendant would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class members' PII, which directly caused the Data Breach;
- Omitting, suppressing, and concealing the material facts that it did not reasonably or adequately secure or monitor it systems to prevent and detect unauthorized access, which directly caused the Data Breach.

130. Defendant's representations and omissions were likely to mislead reasonable consumers about the sufficiency and reasonableness of Defendant's data security and ability to prevent and detect breaches to protect and safeguard Plaintiff's and Class members' PII.

131. Had Defendant disclosed to Plaintiff and Class members that its data systems were not secure and, thus vulnerable to attack, Defendant would have been unable to continue its business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Defendant received, collected, stored, and compiled in easily accessible electronic format Plaintiff's and Class members' PII as part of the services Defendant provided and for which Plaintiff and Class members paid Defendant money.

132. As a result of Defendant's unconscionable, unfair, and deceptive acts and omissions, Plaintiff and Class members have suffered and will continue to suffer foreseeable harm. Plaintiff and Class members have suffered actual damages including, but not limited to, imminent risk of identity theft; expenses and/or time spent on credit monitoring for a period of years; time spent scrutinizing bank statements, credit card statements, and credit reports; time spent initiating fraud alerts and credit freezes and subsequently temporarily lifting credit freezes; and increased risk of future harm. Further, Plaintiff and Class members have suffered and will continue to suffer other forms of injury and/or harm including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

FOURTH CAUSE OF ACTION
Violation of the Ohio Residential Mortgage Loan Act ("RMLA"),
Ohio Rev. Code § 1322.01, *et seq.*
(On behalf of Plaintiff and the Ohio Subclass)

133. Plaintiff repeats and realleges paragraphs 1-103 with the same force and effect as though fully set forth herein.

134. Defendant is a registrant, licensee, and a person required to be registered or licensed under the RMLA.

135. As a registrant, licensee, or person required to be registered or licensed under the RMLA, Defendant cannot "[e]ngage in conduct that constitutes improper, fraudulent, or

dishonest dealings." Ohio Rev. Code § 1322.40(C).

136. In addition, a registrant, licensee, or person required to be registered or licensed under the RMLA is required to comply with all duties imposed by other statutes or common law, act with reasonable skill, care, and diligence and act in good faith and with fair dealing in any transaction, practice, or course of business in connection with the brokering or originating of any residential mortgage loan. Ohio Rev. Code § 1322.45(A).

137. Defendant's failures to implement and maintain reasonable security measures with respect to Plaintiff's and Class members' PII violated the RMLA.

138. As a result of the conduct of Defendant, Plaintiff and Class members have suffered and will continue to suffer foreseeable harm. Plaintiff and Class members have suffered actual damages including, but not limited to, imminent risk of identity theft; expenses and/or time spent on credit monitoring for a period of years; time spent scrutinizing bank statements, credit card statements, and credit reports; time spent initiating fraud alerts and credit freezes and subsequently temporarily lifting credit freezes; and increased risk of future harm. Further, Plaintiff and Class members have suffered and will continue to suffer other forms of injury and/or harm including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

PRAYER FOR RELIEF

WHEREFORE Plaintiff, individually and on behalf of the Classes, requests that the Court:

1. Certify this case as a class action on behalf of the Classes defined above, appoint Plaintiff as the Class representative, and appoint the undersigned counsel as Class counsel;

2. Award declaratory, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class members;

3. Award restitution and damages to Plaintiff and Class members in an amount to be determined at trial;

4. Award Plaintiff and Class members their reasonable litigation expenses and attorneys' fees to the extent allowed by law;

5. Award Plaintiff and Class members pre- and post-judgment interest, to the extent allowable; and

6. Award such other and further relief as equity and justice may require.

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury of any and all issues in this action so triable of right.

Respectfully submitted,

The Advocacy Group
Attorney for Plaintiff
100 S. Biscayne Blvd, Suite 300
Miami, Florida 33131
Telephone: (954) 282-1858
Facsimile: (954) 282-8277
Email: service@advocacypa.com

/s/ Jessica L. Kerr
Jessica L. Kerr, Esq.
Fla Bar No. 92810

DannLaw
Attorney for Plaintiff
Brian D. Flick
15000 Madison Avenue
Lakewood, OH 44107
Telephone: (216) 373-0539
Facsimile: (216) 373-0536
Email: mdann@dannlaw.com
Email: notices@dannlaw.com

/s/ Brian D. Flick
Ohio Bar No. 0081605
(*pro hac vice anticipated*)

Zimmerman Law Offices, P.C.
Attorney for Plaintiff
Thomas A. Zimmerman, Jr.

tom@attorneyzim.com
77 W. Washington Street, Suite 1220
Chicago, Illinois 60602
(312) 440-0020 telephone
(312) 440-4180 facsimile
www.attorneyzim.com
firm@attorneyzim.com

*/s/*Thomas A. Zimmerman, Jr.
Thomas A. Zimmerman, Jr.
(*pro hac vice anticipated*)

The Law Offices of Joseph M. Adams
Attorney for Plaintiff
Joseph M. Adams
Pa. I.D. 58430
200 Highpoint Drive
Suite 211A
Chalfont, PA 18914
Tel: (215-996-9977)
josephmadamsesq@verizon.net

/s/Joseph M. Adams
Joseph M. Adams
(*pro hac vice anticipated*)